Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD

Anthony David Scott and Michael Malloy
Deloitte Consulting, LLP[1]

Peter Clay and Mark Masone
Deloitte & Touche, LLP

As the number of individual service-oriented architecture (SOA) projects going through the certification and accreditation (C&A) process in the DoD increases, it becomes more important to clarify the "unknowns" associated with each component. This article is a starting point for chief information officers, senior information assurance officers (SIAOs), and project managers (PMs) in the DoD, providing an overview of the challenges associated with the C&A process for SOA implementations and outlining eight rules to consider in support of a successful C&A of an SOA implementation.

When faced with the challenges of achieving system C&A in a net-centric environment, today's DoD SIAOs face a new set of challenges—such as *trusting the edge*, implementing SOA solutions, federations, varying degrees of classification levels (CLs), and multiple communities of interest (COI)—that weren't previously faced in siloed, stovepiped, vertical systems. With the discrete information systems of the past, accreditation was generally a better-defined and understood process, given the clear boundaries and finite rules governing the operating environments for such systems; today's environments are more heterogeneous and complex. The details of an SOA implementation are presently not well-defined (see Figure 1). This leaves a high degree of uncertainty and inconsistency unresolved during the first two stages of the C&A process as defined by the DoD Information Assurance Certification and Accreditation Process (DIACAP). These stages are called "Initiate and Plan Information Assurance (IA) C&A" (Stage 1) and "Implement and Validate Assigned IA Controls" (Stage 2) [1].

C&A Challenges for SOA Implementations

Unlike a vertical architecture, a horizontal architecture typically shares modules that relay data to and from other horizontal architectures, allowing the dissemination of information across COI and, at times, differing CLs. For horizontal integration, the approach toward all phases of the C&A process differs from those in a vertical integration because they involve a multiplicity of stakeholders, information systems (ISs), and environments. With that said, PMs need to pay particular attention to the first two stages of the C&A. During Stage 1, the system is registered with the DoD component program, IA controls are assigned, the DIACAP team is assembled, and the DIACAP implementation plan is initiated [1]. During Stage 2, the DIACAP implementation plan is executed, validation activities are conducted, a Plan of Action and Milestones (POA&M) is prepared, and the validation results are compiled into the DIACAP scorecard [1]. It is during these two stages that the most effective savings can be realized based on proper planning and stakeholder involvement, since the costs to remediate weaknesses are lower at this time than they will be when development is further down the road.

The DoD's increasing need to share information across boundaries provides an impetus for promoting a greater use of horizontally integrated systems, and, in turn, the ability to leverage architecture design strategies such as SOA. SOA implementations empower the DoD to achieve significant cost-savings advantages, gained by realizing economies of scale, which results from an architecture that is agile, interoperable, and open to growth. The advantages are realized by enabling information sharing and bridging disparate networks—both highly classified and open coalition.

An SOA implementation is only as secure as the most vulnerable component in the system. Clearly, a failure in effective security design and implementation can result in the significant compromise of mission-critical systems, with devastating effects at the DoD [2]. The reality of the risks, coupled with the deep functional and programmatic complexities associated with accreditation decisions in the SOA environment, have contributed to the view that achieving C&A in an effective and timely manner is an impediment to rapid Global Information Grid/net-centric SOA project rollouts when compared to C&A for traditional systems [3].

As with most high-tech companies in the private sector, the DoD's highly intelligent and well-intentioned leaders are challenged in balancing the competing demands of the *PM triad*: achieving a low-cost, on-time, and high-quality certification determination and accreditation decision for their horizontally aligned SOA implementation. At a high level, some of the programmatic issues facing the DoD are depicted in Table 1 (see next page). Not balancing the four issues could lead to an inability to achieve C&A for SOA with Full Operational Capabilities.

Several aspects of the C&A process for an SOA implementation can be reengineered. From a policy and effective practices viewpoint, a certification determination for SOA implementations is often difficult, in part due to the shifting, dynamic nature of the accreditation boundary itself [4]. Often, after going through a traditional C&A process, the scope of the final SOA implementation is reduced in functionality and implemented in such a manner that it resembles the kinds of stovepiped systems it was intended to supersede, and therefore does not reap the benefits of horizontal integration.

Figure 1: *C&A Process for Vertical and Horizontal Information Systems*

Figure 2 depicts a scenario in which the C&A process avoided complacency and facilitated an agile, robust horizontal architecture; the tendency to not accredit horizontal components limits the DoD from extracting Full Operational Capabilities for their SOA implementation.

In response to the programmatic challenges that confront DoD program managers, eight rules will be outlined (in the following section) for PMs to consider in their efforts to face and resolve the C&A challenges associated with SOA implementations. These rules are not an exhaustive list, but are rather a starting point to detail unique concerns for SOA implementations that are not typical in vertical, siloed, non-SOA implementations.

Eight Programmatic Rules to Consider

In the previous section, we identified the unique risks coupled with the C&A process for SOA associated with late identification of requirements and mitigation approaches due to the dynamic development model. We have witnessed that, all too often, the C&A process for an SOA implementation is prolonged, resulting in huge cost overruns and missed opportunities for early remediation of identified weaknesses. To be successful, there is a need for key PMs from different COIs associated with the SOA to involve themselves in sharing information and to be a part of a dedicated group committed to a successful C&A. This group must focus on consistent coordination of C&A activities and communication among stakeholders in order to fulfill the accreditation process on schedule. The following eight rules are unique to the C&A process for an SOA implementation. One would ask the DoD to consider these, in order, in their efforts to reduce risk and increase the likelihood of a successful C&A for an SOA implementation.

Rule 1: Understand SOA and C&A

As suggested earlier, today's C&A process for SOA implementations has not reached a mature state. The first and most important rule for PMs is to understand SOA and the C&A process. One of many complexities arises from the fact that the DIACAP was not authored with SOA in mind. Information superiority will emerge and productive meetings will take place only when leaders and participants understand the intersections between SOA and C&A.

When leaders do not have a grasp of SOA, unnecessary delays can occur and the functionality of the SOA implementation is at risk of being marginalized or lost completely. If necessary, appropriate briefings or training should be considered as a prerequisite for participating decision-makers.

Rule 2: Embrace Risk Management, Identification, and Planning

Each IS in the DoD is unique and has uncertainties associated with it. Risk management should be performed over the lifetime of the accreditation decision to assess and monitor risk. A POA&M should be used to mitigate the risk of an incident occurring. At the least, the POA&M should detail the priorities of the risk, status, and due date. If PMs do not plan for risk, it is very likely that they will be forced into addressing unexpected issues that may ultimately result in cost overruns and/or undesirable accreditation decisions.

In addition to risk management, risk identification and planning must also be addressed. For C&A of an SOA implementation, risk identification and planning is more involved and less understood than C&A of traditional stovepiped architecture.

Table 1: *Programmatic Issues Facing the DoD*

Scope	Quality	Cost	Schedule
• Dynamic system boundary • Dynamic classification levels • Dynamic services	• Systems not performing as designed • Confusion about who owns services • Managing multiple COI services • Lack of innovation • Lack of training • Nonadherence to policy • High repetition	• Poor execution of acquisition process (DoD 5000 series) • Poor estimation of level of effort (LOE) • Poor capitalization on economics of scale	• Delay in authorization to operate (ATO) • Complacency towards C&A change

It is imperative that the C&A process for SOA implementations is accurately budgeted and appropriately managed to promote reduced risk and avoid cost overruns as SOA components are reworked to address interim weaknesses. From a DoD policy stance, when an SOA implementation is accredited correctly, IA costs go down by an order of magnitude, as do the risks. On paper, the reduction in cost and apparent increase in security is impressive. However, the results are elusive: The IA risk profile of the system actually increases because new security vectors are created within the boundary of the SOA implementation. Extending security beyond what policy mandates and implementing proactive, repeatable procedures into the C&A process should contribute to ensuring a(n) 1) reduction in risk of budget overruns, 2) consistency in planning, and 3) increase in the dissemination of information pertaining to existing risks. Since the systems development life cycle of a horizontal system is heavily dependent on constituents and external partners, unique considerations exist for the C&A process for SOA implementations that rely heavily on teaming and communicating with external parties and internal constituents. Budget overruns can be reduced when security is fully integrated throughout the systems development life cycle and repeatable processes are fully documented and appropriately executed.

If adverse risk is not properly characterized, the C&A process could be forced to continue past the expected timeframe (i.e., the ATO could be pushed back). As a result, resources supporting the C&A process would need to stay on longer, preventing them from being productive on other projects and, if the contract is not fixed price, causing cost overruns on the C&A project. When resources are not able to join other projects, it causes a chain reaction: The critical path of the organization is impacted, and the overall functionality of the organization is reduced. As a result, the project might be completed at a date later than planned, costs might overrun, and the organization's service reputation might slip.

Rule 3: Understand that Schedule and LOE Estimations are Different

Unlike stovepiped systems, an increased LOE needs to be dedicated to educating the IA community on SOA, SOA risks, and SOA protections. As a result, the schedule and LOE is different than that of a traditional vertical IS; it will increase. It has been seen with many new technolo-

gies attempting to go through the C&A process in the DoD. For example, in the wireless arena, much effort has gone into educating the IA community on the risks and protections needed to achieve secure wireless. Similarly, accomplishing the same goals for SOA will tend to increase the required LOE and schedule for the C&A of SOA implementations, at least initially.

In addition to educating the IA community, procedural issues can slow down the C&A process. At present, SOA services themselves cannot be accredited, although there are several proposals and notional constructs on how it could be done currently circulating throughout the DoD community. The future accreditation of services is, by itself, a major topic and not limited to considerations for schedule and LOE.

Rule 4: Plan for Future External Relationships

The goals of SOA include improved collaboration, interoperability, horizontal integration, efficiency, and agility. These goals can be realized only through expanding the IS's boundary to encompass the SOA's multiple accreditation components in a consistent, reusable form.

It is important that PMs plan ahead for interoperability with IA controls of future SOA implementations. Future SOA implementations and shared services with external third parties will have configurations and IA controls that might cause interoperability; anticipation and planning should help avoid this.

PMs for a new SOA must communicate early with owners of other enclaves and COI; the goal is to drive existing ATO dates, anticipate changes to current configurations, and consider controls used in SOA implementations still on the horizon. The goal should be for the overall level of risk associated with the system to be recognized as *acceptable* to the IS that will be exchanging services with the new IS being accredited. It is critical to gather stakeholder risk issue input prior to implementation, otherwise belated input may become a problem for the SOA C&A on the whole.

Rule 5: Plan for Present External Relationships

When operating an IS, the DIACAP limits the time that an accreditation decision is valid based on the severity categories (indicating the risk level associated with the security weakness), expressed as category (CAT) I, CAT II, and CAT III, where CAT I is more severe than CAT III. Sections 4.9 and 6.3.3.2.6 [1] detail the duration associated with Interim Authorization to Operate (IATO), ATO, Interim Authorization to Test (IATT), or Denial of Authorization to Operate decisions. Table 2 provides a summary of the duration of each of these decisions; the duration of an ATO has direct cost and schedule impacts.

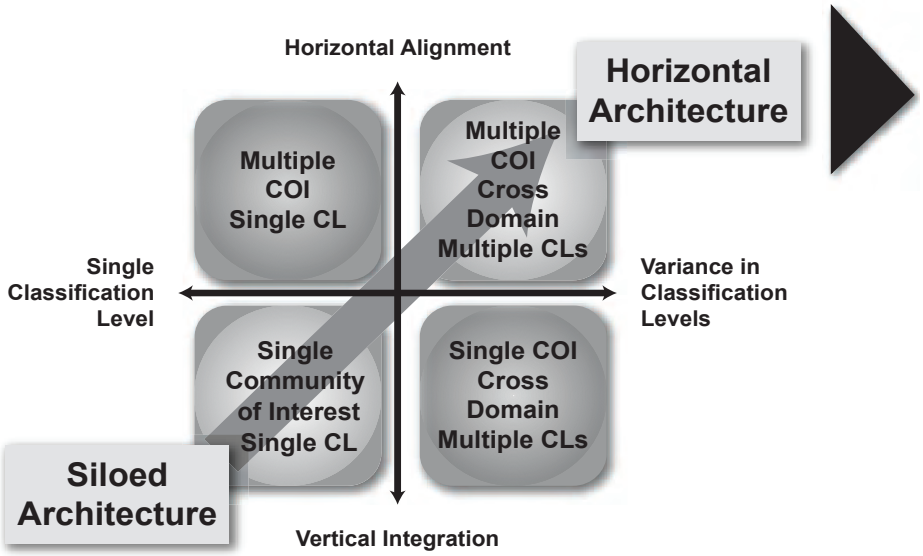

Figure 2: *Sample C&A Process*

Since PMs are responsible for reducing risk and balancing scope, cost, schedule, and quality, an understanding of the duration of each accreditation decision and knowledge about when the ATOs expire is mandatory. This knowledge should also be included in the LOE estimates. As external third-parties' ATOs expire or new service components are added to SOA systems, each service component will have its own corresponding ATO date. If overlooked, these subordinate dates could creep up and possibly impact the overall ATO for the SOA itself.

Each type of accreditation decision (i.e., ATO, IATO, IATT) has a corresponding duration in which the decision is valid. Obviously, longer accreditation periods are preferable in order to reduce the frequency of the accrediting process, which can be costly and impact the system's availability.

The following three factors drive the necessity and urgency behind planning for present-day external third-party relationships:

1. **ATO expiration of existing SOA implementations.** For an existing SOA implementation with shared services from external third parties, it is important to keep track of expiring ATOs to help drive the reaccreditation process, in turn helping ensure shared service availability.
2. **Configuration changes of existing SOA implementations.** For an existing SOA implementation with configuration changes from external third parties, it is important to drive the reaccreditation process, in turn helping ensure shared service availability.
3. **Opportunities to capitalize on economies of scale.** During the C&A process, teaming with organizations might unveil opportunities to eliminate redundant activities and save hard and soft costs.

PMs can begin to experience a decrease in cost overruns by identifying the steps

Table 2: *Duration of the C&A Process*

Type	Authorization Termination Date	CAT I	CAT II	CAT III
ATO	<= 3 years of authorization	No ATO	ATO — must be corrected in 180 days	ATO
IATO	Reset <= 180 of authorization	No ATO	ATO — must be corrected in 360 days	IATO
IATT	Special Case	Special Case	Special Case	Special Case

involved in the C&A process that involve both the organizations they exchange services with, as well as their own organization. Every cost associated with the C&A should be identified, line by line. Once the cost categories have been identified, opportunities for cost savings should be analyzed [5]. An example of cost savings includes teaming with neighboring programs to reduce duplication and eliminate waste. Once waste is identified, PMs should determine what can be realistically eliminated [6].

Rule 6: Use eMASS, DIACAP KS, and Other Cost-Effective or Free Tools

As discussed earlier, PMs should use existing infrastructure tools and knowledge to reduce cost and make quick, measurable progress. Leveraging the DoD's Enterprise Mission Assurance Support Service (eMASS) tool will help automate the DIACAP process via reports generation and tracking of IA controls. The results of the certification determination or accreditation decision are provided automatically on an electronic DIACAP scorecard [7].

DoD organizations can use eMASS for free [8]. Residual costs might include the training of personnel to use eMASS and time to perform data entry. Training and usage costs depend on the number of individuals assigned eMASS roles, locations, facilities, and capabilities. Typically, the cost of training ranges from $5,000 to $10,000 for up to 30 people. Additionally, the Defense Information Systems Agency (DISA) hosts a free quarterly training course, running two full business days.

Like eMASS, DIACAP Knowledge Service (KS) is an information repository that should be leveraged when executing the C&A process for SOA implementations [7]. DIACAP KS holds a wealth of information and up-to-date resources from practitioners that help to facilitate knowledge transfer for the C&A process. For example, the KS houses best practices, lessons learned, guidance documents, schematics, and many other resources to facilitate the DIACAP process [8]. Like eMASS, there is no cost in using KS.

In addition to eMASS and KS, the following are also free IA tools. They should be considered for use during the C&A process for SOA implementations, although many PMs find the tools helpful to support substantially more:

1. **Vulnerability Management System.** A tool developed by the DoD to assess risk during accreditation activities across programs and systems for all types of vulnerabilities.
2. **DoD IT Portfolio Repository – Department of Navy**. A tool developed by the Department of Navy that serves as a technical database of Federal Information Security Management Act assessments.
3. **Gold Disks.** A tool developed by DISA to run vulnerability scans for specific systems, available through the DoD's Information Assurance Support Environment.
4. **Cyber Security Assessment and Management System.** A Web-based tool developed by the Department of Justice that facilitates the C&A process.

Rule 7: Do Not Let Complacency Undermine Horizontal Integration

The DoD systems development environment has been stovepiped for many years. Complacency in moving forward with effective deployment of horizontal integration strategies could ultimately limit the possibilities of an SOA-based enterprise software feature set. Instead of true integration, the DoD could instead wind up with a new series of well-intentioned, but still stovepiped, systems that lack the kind of net-centric data integration and interoperability that has become synonymous with SOA. Complacency results from many things; however, when technology is not well-understood, advanced, or cutting-edge, feature sets may be compromised and replaced with a system that is more familiar, better understood, and more closely resembles the risk profile of past ISs that were accredited. Understandably, a loss of feature sets due to budgetary or mission issues is a business reality. However, if a loss of feature sets is due to an inclination toward not wanting to upset the status quo, it may result in lost opportunity. At a large enough scale, complacency could undermine horizontal integration and the DoD's goal of communicating military intelligence throughout the Global Information Grid and onto the battlefield.

"Governance, interoperability, situational awareness, and data aggregation should be key elements in a fluid maintenance approach to SOA component ATOs."

Rule 8: Strive for a Fluid Maintenance Phase

Maintaining ATO and performing periodic reviews is the fourth phase of the DIACAP process. This compliance phase is an ongoing process that involves vulnerability scans, penetration tests, IA controls verification, scorecard updates, IA controls modifications, security vulnerabilities mitigations, configuration management, and compliance with existing controls. As SOA implementations mature in the DoD, so too will the lessons learned, along with the deepening understanding of SOA's unique IA implications. Governance, interoperability, situational awareness, and data aggregation should be key elements in a fluid maintenance approach to SOA component ATOs.◆

References

1. DoD. *DoD Information Assurance Certification and Accreditation Process*. Instruction 8510.01. 28 Nov. 2007 <www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>.
2. DoD. *Data Sharing in a Net-Centric Department of Defense*. Directive 8320. 02. 23 Apr. 2007 <www.dtic.mil/whs/directives/corres/pdf/832002p.pdf>.
3. Brown, Jeb, and Stacy Spence. "Draft IBM Perspective on Information Assurance Challenges in Service Oriented Architectures." IBM Working Paper. 6 Mar. 2007.
4. "Service-Oriented Architecture." *Wikipedia*. 26 Jan. 2009 <http://en.wikipedia.org/wiki/Service-oriented_architecture>.
5. Dubbeling, Scott, Glenn Richardson, and Brian Siegel. "Strategic Cost Reduction in the Department of Defense." Deloitte eLearning Course. 3 May 2007.
6. "Can We Afford Our Own Future?" *Deloitte Consulting LLP*. 23 Mar. 2009 <www.deloitte.com/dtt/cda/doc/content/us_a&d_project%20management%20report-pov(1).pdf>.
7. Turner, Glenda, et al. "Net-Centric Assured Information Sharing – Moving Security to the Edge Through Dynamic Certification and Accreditation." *IA Newsletter* 8.3. Winter 2005/2006 <http://iac.dtic.mil/iatac/download/Vol8_No3.pdf>.
8. "DIACAP Frequently Asked Questions (FAQs)." *Defense Information Systems Agency*. 4 Apr. 2008 <http://iase.disa.mil/diacap/diacap-faq.pdf>.

Note

1. This publication contains general information only and is based on the experiences and research of practitioners from Deloitte & Touche LLP and Deloitte Consulting LLP, two separate subsidiaries of Deloitte LLP. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Additional Resources

1. Committee on National Security Systems. *National Information Assurance Glossary*. Instruction No. 4009. June 2006 <www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.
2. Project Management Institute. *A Guide to the Project Management Body of Knowledge*. 3rd ed. Newtown Square, PA: Project Management Institute, 2004.
3. DoD. *DoD Information Technology Security Certification and Accreditation Process Application Manual*. Instruction 8510. 1-M. July 2000.
4. DoD. *DoD Information Technology Security Certification and Accreditation Process*. Instruction 5200.40. Dec. 1997.
5. Ross, Ron, et al. *Guide for the Security Certification and Accreditation of Federal Information Systems*. National Institute of Standards and Technology. Special Publication 800-37. May 2004 <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>.
6. National Security Agency – National Security Telecommunications and Information Systems Security Committee. *National Security Telecommunications and Information Systems Security Policy No. 11: National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products*. June 2003.
7. Director of Central Intelligence. *Protecting Sensitive Compartmented Information within Information Systems*. Directive 6/3. 24 May 2000.
8. DoD. *Guidance for Implementing Net-Centric Data Sharing*. Directive 8320.02-G. 12 Apr. 2006 <www.dtic.mil/whs/directives/corres/pdf/832002g.pdf>.
9. Williams, Peter, and Tiffani Steward. "DoD's Information Assurance Certification & Accreditation Process." *Defense AT&L* (Sept.-Oct. 2007).

Software Defense Application

During the C&A process for SOA implementations, the DoD community is given a second chance to solve technical issues that involve software interoperability and security. When the C&A process for an SOA implementation is prolonged, huge cost overruns and missed opportunities can result. This article is a resource and provides the DoD software community with techniques and methodologies to consider in their efforts to avoid unnecessary cost overruns associated with the C&A process for SOA implementations. It ties software selection and security architecture to upfront planning, helping PMs as they streamline the C&A process and reduce costs, risks, and the time to implement—while increasing mission effectiveness.

About the Authors

Anthony David Scott is a manager for Deloitte Consulting with 10 years of cybersecurity experience in the commercial and federal sectors. Scott continues to be an active participant in the federal community, publishing and holding workshops at the IEEE, Computer Security Institute, DoD, and at DHS conferences. He is a licensed professional engineer and a Certified Information Systems Security Professional. Scott holds a master's degree in electrical and computer engineering from Georgia Tech and an MBA from Columbia University.

Deloitte Consulting, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 251-1696
Fax: (703) 332-7108
E-mail: davidscott@deloitte.com

Michael Malloy is an analyst with Deloitte Consulting and works primarily in the public sector with the DoD. He specializes in custom system development and has strong knowledge regarding SOA and related topics. Malloy graduated from Boston College with a bachelor's degree in computer science and mathematics.

Deloitte Consulting, LLP
1001 G ST
STE 900 W
Washington, D.C. 20001
Phone: (443) 694-1545
Fax: (202) 661-1802
E-mail: mimalloy@deloitte.com

Peter Clay is a senior manager with 16 years of IA experience in the federal and financial market sectors. He currently specializes in DoD information security governance and is the federal representative in the Deloitte & Touche Vulnerability Management Center of Excellence. Clay is also a Certified Information Systems Security Professional.

Deloitte & Touche, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 220-3531
Fax: (703) 894-9191
E-mail: peclay@deloitte.com

Mark Masone is a senior manager with nine years experience as an IA professional working closely with federal and DoD organizations. Most notably, he supported the Office of the Assistant Secretary of Defense for Networks and Information Integration on DIACAP implementation efforts. He has supported the authorship of the DIACAP while managing its two components: KS and eMASS. Masone is a Certified Information Systems Security Professional, a Certified Information Privacy Professional/Government, and a Certified Secure Software Lifecycle Professional. He has a bachelor's degree from Virginia Tech and master's degree in systems engineering from George Washington University.

Deloitte & Touche, LLP
1750 Tysons BLVD
McLean, VA 22102
Phone: (703) 251-1843
Fax: (703) 894 -9191
E-mail: mmasone@deloitte.com